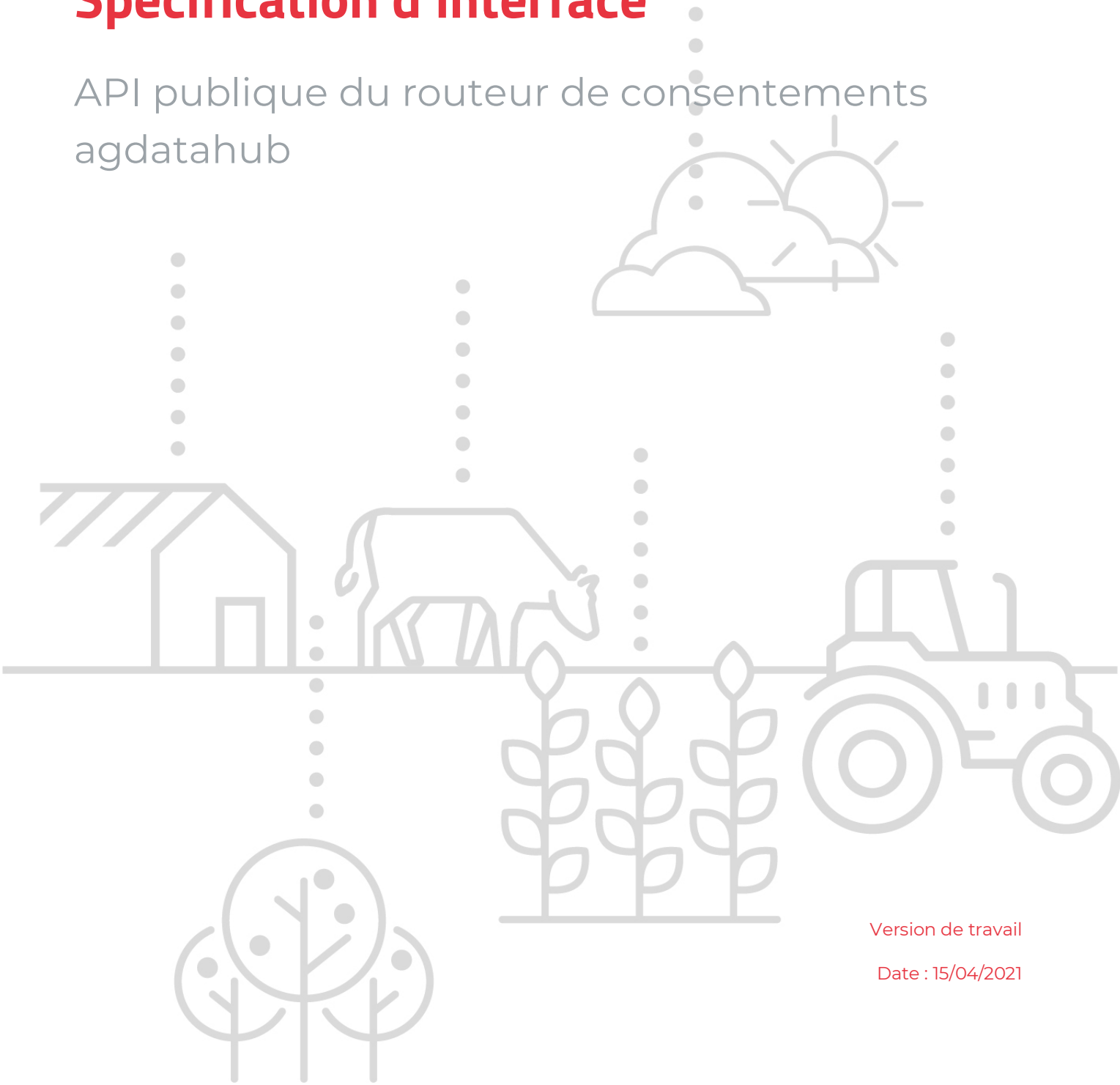
Spécification d'interface

API publique du routeur de consentements agdatahub



Version de travail

Date : 15/04/2021

Sommaire

Description du document

Emetteur	Agdatahub
Projet	Routeur de consentements agdatahub
Nom du document	Routeur_agdatahub_spécification_interfaçage_utilisateur_v1.1
Version	1.1 Version de travail
Rédacteurs	Edouard HUE, OBS Lauréna GENDRE, pour agdatahub

Historique des versions

Version	Opération	Nom	Date
1.0	Création	Edouard HUE	22/03/2021
1.1	Modifications, ajout de contenu	Lauréna GENDRE	15/04/2021

1 Préambule

1.1 Objet du document

Ce document décrit le protocole d'interfaçage des utilisateurs au routeur de consentements agdatahub. Il complète et précise le contrat d'interface « API des consentements agdatahub» au format Open API 3 référencé ci-dessous.

Le dossier de spécification d'interface comprenant ce document et le contrat d'interface Open API 3 a pour but de décrire les modalités d'interfaçage d'un système utilisateur au routeur agdatahub.

1.2 Documents de référence

Titre	Référence	Version
API des consentements agdatahub	consent- api.yaml	1.0.0

1.3 Glossaire des termes utilisés

Termes Utilisés	Description
SGC	Système de gestion des consentements = système d'information qui stocke et gère des consentements
Ayant droit	La personne morale qui a les droits sur les données et dont le consentement est nécessaire
Fournisseur de services bénéficiaire	L'organisme qui propose du service aux agriculteurs et pour ce faire à besoin d'accéder à des données. C'est le bénéficiaire du consentement.
Fournisseur de données	La société en maitrise de la base de données qui fournit les données au fournisseur de services bénéficiaire.
Responsable d'enregistrement du consentement	L'organisme qui enregistre le consentement dans le système informatique d'un gestionnaire de consentements.

2 Fonctionnement général de l'interface avec le routeur agdatahub

2.1 Présentation du système

Le routeur agdatahub joue un rôle de façade en avant des systèmes de gestion des consentements (SGC) tiers participants. Le routeur définit une représentation commune permettant de décrire les consentements de façon indépendante des SGC.

Pour interroger le routeur, les systèmes utilisateurs doivent mettre en œuvre les interfaces définies dans le contrat d'interfaçage. Ces interfaces comprennent l'API de consultation des consentements proprement dite (vérification et récupération de consentements) et une API d'authentification.

Les nouveaux utilisateurs sont enregistrés dans le routeur par l'administrateur Agdatahub. Il convient donc de prendre contact avec agdatahub pour l'inscription et l'utilisation du routeur.

2.2 Concepts d'implémentation

L'API est conçue dans l'optique des respecter les principes RESTful. Elle s'appuie sur les différents verbes du protocole HTTP et utilise le format JSON pour représenter les données. Elle expose une ressource « consents » sur laquelle sont réalisables les opérations HTTP HEAD (vérification de consentements) et GET (récupération de consentements). Les entités nommées sont, dans la mesure du possible, identifiées par des URI.

Lorsqu'un critère optionnel n'est pas renseigné dans une requête, il est ignoré. Il n'est pas prévu de permettre la construction d'un critère portant sur une valeur nulle ou non renseignée.

Les points d'accès sont accessibles uniquement en HTTPS. Le certificat est valide en tout point et est signé par une autorité de certification reconnue par le programme de certification de Mozilla.

3 Description détaillée des services

3.1 Service d'authentification

L'utilisation du routeur nécessite une authentification préalable. Chaque utilisateur du routeur doit être inscrit par l'administrateur AgDataHub et se voit fournir des identifiants permettant cette authentification.

3.1.1 Protocole d'authentification

Le routeur met en œuvre le protocole OAuth 2. Les utilisateurs réalisent une requête de type client credentials grant pour obtenir un jeton d'accès, qu'ils incluent dans chaque requête au routeur sous forme d'un Bearer Token.

3.1.2 Points d'accès

Le routeur supporte OpenID Connect Discovery 1.0. Dans ce cas, seul l'*issuer URI* est nécessaire au client. Pour les clients qui préfèrent une configuration explicite, les URL du *token endpoint* et du *JWK Set* sont décrites ci-dessous.

Plateforme de recette

Clé	Valeur
issuer URI	`https://iam.recette.agri-consent.eu/auth/realms/agri-consent`
token endpoint	`https://iam.recette.agri-consent.eu/auth/realms/agri-consent/protocol/openid-connect/token`
JWK Set	`https://iam.recette.agri-consent.eu/auth/realms/agri-consent/protocol/openid-connect/certs`

3.1.3 Scopes

L'accès au routeur est contrôlé par le mécanisme des scopes OAuth 2. Les clients doivent demander, lors de leur authentification, l'inclusion des scopes correspondant aux actions qu'ils doivent réaliser dans le token qui leur est accordé.

Le scope offline permet d'obtenir un refresh token en plus de l'access token. Ce refresh token peut être utilisé pour renouveler l'access token au lieu de refaire une authentification complète. Il est recommandé de renouveler l'access token à 75 % de sa durée de vie.

3.1.3.1 Accès aux opérations

Les utilisateurs doivent demander explicitement un *scope* correspondant aux opérations qu'ils souhaitent réaliser. Si ce *scope* leur a été accordé lors de leur inscription, il sera ajouté au jeton. Sinon, la demande sera rejetée.

Scopes d'accès aux opérations

Opération	*Scope*
Récupération de consentements	`urn:agdatahub:agri-consent.eu/consents/get`
Vérification de consentement	`urn:agdatahub:agri-consent.eu/consents/check`

3.1.3.2 Accès aux données

Chaque système acteur interrogeant le routeur est enrôlé par l'administrateur agdatahub avec un rôle dédié et un protocole sécurisé est utilisé pour les échanges OIDC. Le routeur joue le rôle de tiers de confiance et les restrictions opérées en entrée du routeur sont les suivantes :

- Un fournisseur de service bénéficiaire ne peut récupérer ou vérifier en tant que bénéficiaire que les consentements pour lesquels il est bénéficiaire (son propre SIRET est renseigné dans le paramètre serviceProvider)
- Un fournisseur de données ne peut récupérer ou vérifier en tant que fournisseur de données que les consentements pour lequel il est fournisseur de données (son propre SIRET est renseigné dans le paramètre dataSupplier) et les consentements donnés pour tous les fournisseurs de données
- Un responsable d'enregistrement ne peut récupérer en tant que responsable d'enregistrement que les consentements pour lesquels il est responsable d'enregistrement (son propre SIRET est renseigné dans le paramètre collector)

Ces trois rôles (fournisseur de service bénéficiaire, fournisseur de données, responsable d'enregistrement) sont représentés par autant de *scopes*. L'un de ces rôles (ou une combinaison) est affectée au système utilisateur lors de son inscription. Le système utilisateur doit demander explicitement **un seul** de ces scopes lors de son authentification. Il pourra alors de consulter les consentements qui le concerne en indiquant son n° de Siret dans le critère associé au *scope* demandé.

Scopes d'accès aux données :

Rôle	Scope	Paramètre
Bénéficiaire	urn:agdatahub:agri-consent.eu/third-party/service-provider	serviceProvider

Fournisseur de services		
Fournisseur de données	urn:agdatahub:agri-consent.eu/third-party/data-supplier	dataSupplier
Responsable d'enregistrement	urn:agdatahub:agri-consent.eu/third-party/collector	collector

Il n'est pas permis d'utiliser un jeton portant simultanément plusieurs de ces scopes.

3.2 API de consultation des consentements

Cette API expose deux fonctionnalités : le test de l'existence d'un consentement (vérification de consentement /check consent) et la recherche de consentements (récupération de consentements / get consent).

3.2.1 Description du service de vérification des consentements

Ce service permet de vérifier l'existence d'un consentement auprès de tous ou certains gestionnaires de consentements connectés au routeur. Le consentement est décrit par les paramètres d'entrée. Cette vérification peut par exemple être réalisée en amont d'un transfert de données.

Le service est exposé en HEAD.

3.2.1.1 Paramètres transmis en entrée

Paramètre	Description	Type	Cardinalité	Obligatoire
dataSupplier	Fournisseur des données sujettes aux consentements.	n°SIRET	0..1	non
rightHolder	Ayant-droit ayant accordé des consentements.	n° SIRET n° NUMAGRIT n° EDE	1	oui
serviceProvider	Fournisseur de services bénéficiaire des consentements	n°SIRET	1	oui

family	Famille(s) de données concernée(s) par les consentements	Chaine de caractères	1..20	oui
usage	Usage consenti sur la/les famille(s) de données.	Chaine de caractères	1	oui
consentManager	Gestionnaires des consentements (code)	Chaine de caractères	0..n	non

3.2.1.2 Description des réponses

Code	Description
200	Vérification réussie, il existe au moins un consentement répondant aux critères chez un gestionnaire de consentements interrogé. Les réponses de certains gestionnaires ont pu être ignorées.
204	Vérification réussie, mais il n'existe aucun consentement répondant aux critères chez les gestionnaires interrogés.
400	Requête incohérente.
401	Authentification absente ou invalide.
403	Droits de l'utilisateur insuffisants.
504	Parmi les gestionnaires interrogés, au moins un gestionnaire n'a pas répondu et aucun n'a indiqué qu'il existait un consentement répondant aux critères.

3.2.1.3 Précisions

Numéro	Description	Exemples
1	La vérification d'un consentement vise à déterminer si un usage spécifique est consenti. Cet usage peut être permis par un consentement accordé sur un plus large périmètre (bénéficiaires, fournisseurs de	Il existe chez un SGC un consentement accordé pour un usage u1 sur les familles de données f1 et f2. La vérification du consentement à l'usage u1 sur la seule famille f1 a donc un résultat positif.

	données, familles de données). Dans ce cas, la réponse attendue est positive.	De la même manière, s'il existe un consentement accordé pour les usages u1 et u2 sur la famille f1, la vérification du consentement au seul usage u1 sur la famille f1 a un résultat positif.
2	Tous les aspects du consentement recherché doivent être précisés, à l'exception du fournisseur de données qui peut être omis.	
3	Si le paramètre fournisseur de données n'est pas renseigné (champ optionnel), la réponse est négative si le consentement a été donné de manière restrictive pour un fournisseur de données en particulier.	Il existe des consentements chez un SGC portant sur un fournisseur f2 de manière restrictive. Si la vérification de consentement ne mentionne pas de fournisseur de données explicitement, alors la réponse est négative.
4	Plusieurs familles de données peuvent être incluses dans les critères de recherche. Le consentement est vérifié séparément pour chacune des familles précisées. Une réponse positive garantit que l'usage demandé est consenti pour chacune des familles, même si le consentement est fragmenté chez différents SGC.	
5	La vérification de consentement est réalisée pour la date et l'heure courante à la réception de la requête. Une réponse positive est valable à l'instant de se réception mais ne précise en rien la durée de sa validité.	
6	Il est possible de restreindre la recherche de consentements à un ou plusieurs gestionnaires de consentements explicitement précisés en indiquant leur code dans le parameter consentManager. Sans précision, tous les gestionnaires de consentements connus du système sont interrogés.	

7	Une réponse positive à une vérification de consentement indique qu'il existe au moins un consentement chez un gestionnaire. Certains gestionnaires ont pu ne pas avoir été interrogés.	
8	À l'inverse, une réponse négative garantit que tous les gestionnaires ont été interrogés et ont tous répondu négativement.	
9	Si au moins un gestionnaire échoue à répondre et si tous les autres gestionnaires répondent négativement, le routeur ne peut déterminer si le consentement est accordé et répond par un code d'erreur spécifique. La requête peut être retentée ultérieurement.	

3.2.2 Description du service de récupération des consentements

Ce service permet de récupérer une liste de consentements conformes aux paramètres transmis en entrée.

La récupération de consentements recherche auprès des gestionnaires et agrège les consentements satisfaisant aux critères demandés.

Le service est exposé en GET.

3.2.2.1 Paramètres transmis en entrée

Aucun critère n'est obligatoire mais au moins un critère de type acteur (dataSupplier, rightHolder, serviceProvider, collector) doit être spécifié.

Paramètre	Description	Type	Cardinalité	Obligatoire
dataSupplier	Fournisseur des données sujettes aux consentements.	n°SIRET	0..1	non
rightHolder	Ayant-droit ayant accordé des consentements.	n° SIRET n° NUMAGRIT	0..1	non

serviceProvider	Fournisseur de service bénéficiaire des consentements	n°SIRET	0..1	non
collector	Responsable de l'enregistrement des consentements	n°SIRET	0..1	non
family	Famille(s) de donnée(s) concernées par les consentements	Chaine de caractères	0..20	non
usage	Usage consenti sur la/les famille(s) de donnée(s).	Chaine de caractères	0..1	non
consentManager	Gestionnaires des consentements	Chaine de caractères	0..n	non
activeAt	Moment auquel les consentements renvoyés doivent être actifs	Date heure	1	oui

3.2.2.2 Description des réponses

Code	Description
200	Succès, tous les consentements répondant aux critères sont renvoyés. ➔Envoi de la liste de consentements au format JSON
204	Succès, mais il n'y a aucun consentement correspondant aux critères demandés. Tous les gestionnaires de consentement interrogés ont répondu.
400	Requête incohérente. ➔Détail de l'erreur
401	Authentification absente ou invalide.
403	Droits de l'utilisateur insuffisants. Détails

504	Échec partiel : tous les gestionnaires de consentement n'ont pas répondu ou certaines gestionnaires ont remontés des données invalide non routées par le routeur. Seuls les consentements fournis par les gestionnaires ayant répondu correctement sont inclus dans la réponse. La liste peut être vide. Il peut néanmoins exister des consentements chez les gestionnaires n'ayant pas répondu. Les gestionnaires n'ayant pas répondu ou ayant répondu avec des données invalides sont précisés dans la réponse. Si l'erreur se reproduit, il convient de se rapprocher du support agdatahub.

3.2.2.2.1 Description d'un consentement

Le tableau ci-après présente **à titre informatif** les données de description d'un consentement. Le format JSON précis pour la restitution des données de consentement est celui présenté dans le contrat d'interface Open API 3 joint à ce document.

Champs	Description	Type	Obligatoire
id	Identifiant du consentement. Cet attribut identifie le consentement parmi ceux sous la reponsabilité de son gestionnaire. Cet identifiant ne doit pas être considéré comme globalement unique.	Chaine de caractère	oui
Informations liées aux acteurs autour du consentement			
rightHolder	Identifiant de l'ayant droit ayant donné son consentement	SIRET NUMAGRIT	oui
serviceProvider	Identifiant du ou des fournisseur(s) de services bénéficiaire(s) du consentement.	SIRET	oui
dataSupplier	Identifiant du fournisseur de données.	SIRET	non
collector	Identifiant du responsable d'enregistrement.	SIRET	oui
additionalIdentifier	Identifiant complémentaire relatif au consentement.	EDE	non

consentManagerId	Code du gestionnaire de consentement duquel provient le consentement remonté.	Chaine de caractère	oui
Informations liées à l'usage permis des données			
id	Identifiant d'un cas d'usage	Chaine de caractère	oui
label	Libellé du cas d'usage	Chaine de caractère	oui
description	Description de l'usage autorisé en texte libre (non normalisé).	Chaine de caractère	non
constraints	Liste des contraintes applicables à ce consentement. Une liste vide équivaut à une liste nulle.	Liste	non
additionalRestrictions	Restrictions supplémentaires en texte libre	Chaine de caractère	non
Informations liées aux données pour lesquelles le consentement est accordé			
id	Identifiant d'une famille de données.	Chaine de caractères	oui
label	Libellé pour cette famille.	Chaine de caractères	oui
Informations liées à la période de validité du consentement			
begin	Date d'entrée en validité.	Date/heure	oui
end	Date d'expiration	Date/heure	non
Information liée au contrat duquel peut dériver le consentement			
contract	Référence permettant d'identifier ce contrat, quand elle est connue.	Chaine de caractères	non

3.2.2.3 Précisions

Numéro	Description	Exemples
1	Les critères sont combinés par le routeur avec un ET logique. Chaque consentement renvoyé satisfait donc chacun des critères.	_
2	La description des consentements renvoyée en réponse à une requête est exhaustive et indépendante des critères de recherche: la réponse est complète quels que soient les paramètres d'entrée. Tous les attributs sont renseignés avec toutes les valeurs prises pour le consentement représenté.	_
3	Lorsque le consentement a été donné quelque soit le fournisseur de données, les consentements sont réputés être accordés à tout fournisseur de données et l'identifiant réservé à cet usage est utilisé dans la représentation des consentements « urn:agdatahub:agri-consent.eu/data-supplier/any ».	Il existe des consentements chez un SGC qui ont été accordés quelque soit le fournisseur de données. Pour ce SGC et les consentements concernés : Une requête portant sur le fournisseur f1 a pour résultat tous les consentements correspondant aux autres critères de la requête. Les consentements renvoyés sont indiqués comme valables pour tous les fournisseurs de données. Une requête sans critère de fournisseur de données a pour résultat tous les consentements correspondant aux autres critères de la requête. Les consentements renvoyés sont indiqués comme valables pour tous les fournisseurs de données.
4	La description des consentements renvoyée en réponse à une requête est exhaustive et indépendante des critères de recherche (la réponse est complète	Il existe chez un SGC un consentement pour l'usage u1 sur les familles de données f1 et f2. En réponse à une recherche de

	quelque soient les paramètres d'entrée). Tous les attributs sont renseignés avec toutes les valeurs prises pour le consentement représenté.	consentements pour l'usage u1 sur la famille f1, le SGC retourne ce consentement en indiquant qu'il est donné pour les deux familles f1 et f2.

3.2.3 Principes communs aux 2 services

3.2.3.1 Nommage des entités

Cette section décrit la manière dont les entités nommées sont identifiées dans le contrat d'interface. Le principe général est de représenter les entités nommées par des URN afin d'éviter les collisions et de permettre une extension à de nouvelles entités.

On prévoit un espace de nommage propre à Agdatahub nommé « agdatahub ». Cet espace de nommage ne fait pas l'objet d'un dépôt formel à l'IANA pour le moment.

3.2.3.1.1 Numéros de Siret

Les numéros de Siret sont représentés par un URN dans l'espace de nommage agdatahub. Au sein de l'espace de nommage, ils sont identifiés par le préfixe SIRET:.Le numéro SIRET est directement accolé à ce préfixe.

Exemple : urn:agdatahub:SIRET:42226020800026

Les numéro de SIRET sont contrôlés par le routeur au travers de l'algorythme de Luhn. Une mauvaise configuration sur un numéro de SIRET peut donner lieu à une réponse de type "Requête incohérente". Le detail de l'erreur est précisé dans la réponse du routeur.

3.2.3.2 Numéros Numagrit

Les numéros Numagrit sont représentés par un URN dans l'espace de nommage agdatahub. Au sein de l'espace de nommage, ils sont identifiés par le préfixe NUMAGRIT:. Le numéro Numagrit est directement accolé à ce préfixe.

Exemple urn:agdatahub:NUMAGRIT:A73001002001

La conformité de nomenclature des Numagrit est contrôlée par le routeur. Une mauvaise configuration sur un Numagrit peut donner lieu à une réponse de type "Requête incohérente". Le detail de l'erreur est précisé dans la réponse du routeur.

3.2.3.3 Numéros EDE

Les numéros EDE (Établissement de l'élevage) sont représentés par un URN dans l'espace de nommage agdatahub. Au sein de l'espace de nommage, ils sont identifiés par le préfixe EDE:. Le numéro EDE est directement accolé à ce préfixe.

Exemple urn:agdatahub:EDE:123456

La conformité de nomenclature des numéro EDE n'est pas contrôlée par le routeur.

3.2.3.4 *Identification des acteurs*

Les acteurs sont identifiés par des attributs spécifiques à leur situation. Ces attributs sont représentés selon le formalisme décrit précédemment.

Ayant-droits

Les ayant-droits sont identifiés par leur n° de Siret, n Numagrit ou n°EDE.

Responsables d'enregistrement

Les responsables d'enregistrement sont identifiés par leur n° de Siret.

Fournisseurs de services

Les fournisseurs de service sont identifiés par leur n° de Siret.

Fournisseurs de données

Les fournisseurs de données sont identifiés par leur n° de Siret.

Cas spécifiques

Lorsqu'un consentement est valable pour n'importe quel fournisseur de données, cet identifiant réservé est utilisé à la place de l'identifiant du fournisseur de données : « urn:agdatahub:agri-consent.eu/data-supplier/any ».

3.2.3.5 *Référentiel*

La version actuelle du système est une première version n'intégrant pas de normalisation des référentiels. Il est prévu qu'un travail d'harmonisation des référentiels (usages, familles de données, contraintes d'usage) soit réalisé dans le cadre du projet NUMAGRI. Cette harmonisation des référentiels aura un impact sur la représentation des données ci-dessous (codification partagée).

3.2.3.5.1 Contraintes d'usage

La représentation des contraintes d'usage ne fait l'objet d'aucune normalisation dans cette version du système. Leurs identifiants sont formés d'une suite de caractères sans formalisme particulier.

3.2.3.5.2 Familles de données

La représentation des identifiants des familles de données ne fait l'objet d'aucune normalisation dans cette version du système. Leurs identifiants sont formés d'une suite de

caractères sans formalisme particulier. Le label soit être renseigné pour affichage dans le portail Agri-consent.

Exemples : Données d'élevage

3.2.3.5.3 Catégories d'usage

Les catégories d'usage ne font l'objet d'aucune normalisation dans cette version du système. Leurs identifiants sont formés d'une suite de caractères sans formalisme particulier.

Exemples : Mesure de la performance